AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1-27. (Canceled)

28. (New) A computer emergency response system linked to a plurality of computer systems, the system comprising:

an information section configured to collect system information for at least one of the plurality of computer systems and security information related to one or more security incidents that are a threat to at least one of the plurality of computer systems;

a test bed configured to perform a simulation under a similar condition of at least one of the plurality of computer systems based on the system information and security information; and

an assessment section configured to assess the one or more security incidents based on the simulation.

29. (New) The computer emergency response system of claim 28, wherein the test bed resides on a different computer system than the at least one simulated computer system.

30. (New) The computer emergency response system of claim 28, wherein the assessment section assesses the one or more security incidents by classifying the one or more security incidents into one or more levels of attack.

31. (New) The computer emergency response system of claim 30, further comprising an evaluation section configured to calculate expected damages from an attack based on at least one security incident with a similar level of attack.

32. (New) The computer emergency response system of claim 31, further comprising an asset recovery section configured to provide an expected recovery time from the attack for at least one of the plurality of computer systems.

33. (New) The computer emergency response system of claim 30, wherein the assessment section is further configured to provide a possible scenario for an attack on at least one of the plurality of computer systems.

34. (New) The computer emergency response system of claim 30, wherein the assessment section is further configured to use the test bed to automatically assess the one or more security incidents.

35. (New) The computer emergency response system of claim 30, further comprising an information sharing section configured to classify the security information and transfer the classified security information to at least one of the plurality of computer systems.

36. (New) The computer emergency response system of claim 28, further comprising a warning section configured to issue an alert to the simulated computer system based on an assessment of the one or more security incidents by the assessment section.

37. (New) The computer emergency response system of claim 28, further comprising a warning section configured to issue a forecast to the simulated computer system based on an assessment of the one or more security incidents by the assessment section.

38. (New) A method of simulating an attack in a computer emergency response system that is linked to a plurality of computer systems, the method comprising:

collecting system information for at least one of the plurality of computer systems and security information related to one or more security incidents that are a threat to at least one of the plurality of computer systems;

configuring a test bed under a similar condition of at least one of the plurality of computer systems; and

performing an attack assessment for the one or more security incidents using the test bed.

39. (New) The method of claim 38, wherein the simulation is performed on a different computer system than the at least one simulated computer system.

40. (New) The method of claim 38, wherein the attack assessment classifies the one or more security incidents into levels of attack.

41. (New) The method of claim 40, further comprising calculating expected damage to one or more of the plurality of computer systems from an attack based on at least one security incident with a similar level of attack.

42. (New) The method of claim 41, further comprising calculating an expected recovery time from the attack for at least one of the plurality of computer systems.

43. (New) The method of claim 41, further comprising calculating an expected recovery time from the attack for at least one of the plurality of computer systems.

44. (New) The method of claim 38, further comprising providing a possible scenario for an attack on at least one of the plurality of computer systems.

45. (New) The computer emergency response system of claim 38, wherein the performing of the attack assessment is performed automatically for the one or more security incidents.

46. (New) The computer emergency response system of claim 38, further comprising classifying the security information and transferring the classified security information to at least one of the plurality of computer systems.

47. (New) The computer emergency response system of claim 38, further comprising issuing an alert to the simulated computer system based on the attack assessment.

48. (New) The computer emergency response system of claim 38, further comprising issuing a forecast to the simulated computer system based on the attack assessment.

49. (New) A computer readable medium having stored thereon computer executable components, the medium comprising:

an assessment section configured to provide an assessment which evaluates and classifies security information related to at least one security incident; and

a test bed section configured to simulate an attack on one or more other computing systems networked with a computing device based on the assessment and provide simulation results.

50. (New) The computer readable medium of claim 49, further comprising a security section configured to protect the computing device from the one or more other computing systems based on the simulation results.

51. (New) The computer readable medium of claim 49, wherein the attack simulation is further based on a database of security vulnerabilities of the one or more other computing systems.

52. (New) The computer readable medium of claim 51, wherein the attack simulation determines whether the security vulnerabilities of the one or more other computing systems can be exploited based on the assessment.

53. (New) The computer readable medium of claim 49, wherein the assessment is based on a frequency which the at least one security incident occurs.

54. (New) The computer readable medium of claim 49, wherein the assessment is based on a comparison of the at least one security incident with other security incidents.

55. (New) The computer readable medium of claim 49, further comprising a collection section configured to collect the security information from the one or more other computing systems.

56. (New) The computer readable medium of claim 49, further comprising an information sharing section configured to send the assessment to at least one of the other computing systems.

57. (New) The computer readable medium of claim 49, further comprising an information sharing section configured to send the simulation results to at least one of the other computing systems.

58. (New) The computer readable medium of claim 49, wherein the at least one security incident relates to cyber terror.

59. (New) A computer implemented method comprising:

determining an asset value for a computing device on a network; and

providing a damage calculation for a simulated attack on the computing device based on security information related to a security incident and the asset value.

60. (New) The computer implemented method of claim 59, further comprising outputting the damage calculation to a display.

61. (New) The computer implemented method of claim 59, wherein the security information comprises a likelihood of the security incident occurring.

62. (New) The computer implemented method of claim 59, wherein the damage calculation is provided in monetary units.

63. (New) The computer implemented method of claim 59, wherein the damage calculation provides an estimate of an amount of damage to the computing device from the simulated attack.

64. (New) The computer implemented method of claim 59, wherein the security incident relates to a hacking.

65. (New) The computer implemented method of claim 59, wherein the security incident relates to a worm.

66. (New) The computer implemented method of claim 59, further comprising collecting the security information from one or more other computing systems on the network.

67. (New) The computer implemented method of claim 59, further comprising:

determining a second asset value for a second computing device on the network; and

providing a second damage calculation for the simulated attack on the second computing device based on the security information and the second asset value.

68. (New) The computer implemented method of claim 67, further comprising outputting the damage calculation and second damage calculation to a display.

69. (New) A computer implemented comprising:

simulating an attack on a computing system based on a security vulnerability of the computing system and an exploit to the security vulnerability; and

generating a risk level for the computing system based on the simulation of the attack and an asset value of the computing system.

70. (New) The computer implemented method of claim 69, wherein the security vulnerability comprises a service available on the computing system.

71. (New) The computer implemented method of claim 69, wherein the security vulnerability comprises an application available on the computing system.

72. (New) The computer implemented method of claim 69, wherein the asset value relates to the significance of the computing system.

73. (New) The computer implemented method of claim 69, further comprising protecting the computing system based on the simulation of the attack.

74. (New) The computer implemented method of claim 69, further comprising protecting a second computing system networked with the computing system based on the simulation of the attack.